



Breaking Through the Dissimilar Hardware Restore Challenge

Breaking Through the Dissimilar Hardware Restore Challenge

Contents

Hardware failure is inevitable	4
Automated system recovery	4
Manual system recovery	4
Duplicate hardware for disaster recovery	6
Hardware-independent restore, a critical component of system recovery	6
The Restore Anywhere capability enabling recovery to dissimilar physical computers	7
Restore Anywhere and recovery to virtual computer environments	9
Restore Anywhere for hardware migration and hardware repurposing	10
Hardware migration strategies	10
Repurposing hardware for optimal resource utilization	12
A new option for meeting strict RTOs and upping disaster tolerance	13
Defining “disaster tolerance”	14
What is your Recovery Time Objective (RTO)	15
Conclusion	15

Breaking Through the Dissimilar Hardware Restore Challenge

When Symantec Backup Exec™ System Recovery (formerly Symantec LiveState™ Recovery) was first released, it changed the way that bare metal system recovery was performed for Windows® systems, making it rapid, simple, and reliable. Now with the latest release and the Restore Anywhere capability, Backup Exec System Recovery enables unprecedented speed and ease of recovery to dissimilar hardware platforms.

Hardware failure is inevitable

To combat the erosion of data and the failure of systems, backup procedures must be designed to account for the eventual failure of a computer's hardware. Computer hardware has a finite lifetime. And electronic media is transitory because it must continually be juggled from one storage device to another during its lifetime. While many system failures do not involve hardware failure, those that do must still be addressed in a timely and cost-effective manner. Even if the hardware must be replaced, the need for a rapid system recovery solution exists. Bare metal recovery has two major approaches: automated and manual. Each approach has its uses.

Automated system recovery

Automated bare metal recovery is designed for rapid, systematic recovery. By using automation, procedures are more likely to be predictable and simple. The user will not require as much training, and therefore, the automation approach should also be more reliable. Automated Windows system recovery does, however, have limitations. Because an operating system, with its unique configuration, is designed at the time of installation for a specific hardware device, an automated recovery cannot account for dissimilar hardware components at the core of the new computer system.

The most problematic components are the Windows HAL, or Hardware Abstraction Layer; the kernel; and storage controllers. When a Windows system boots, these three elements must be correctly assigned to the hardware, or Windows will not boot. Solving additional device conflicts are less critical because, once loaded, Windows makes these devices easy to detect and install.

Manual system recovery

Because of the dissimilar hardware limitations of an automated recovery, many users choose a manual reinstallation of the operating system. For instance, in the past when one of the key hardware components failed—storage controller, motherboard, processor, HBA—manual recovery was the only viable approach. By reinstalling the operating system manually, each of these items will be detected and installed in a clean environment. The drawback, of course, is that the system must now be configured entirely from scratch. Service packs and hot fixes must be applied.

“LiveState Recovery brings critical systems back online faster and makes the IT administrator's job easier—and it reduces the road warrior's nightmare to an inconvenience.”

*Dianne McAdam
Senior Analyst & Partner
Data Mobility Group (DMG)*

Breaking Through the Dissimilar Hardware Restore Challenge

Applications must be installed and configured. System settings must be set to match company standards. All this before restoration of data can begin. The complexity of this process is beyond ad hoc management techniques and requires strict controls and procedures.

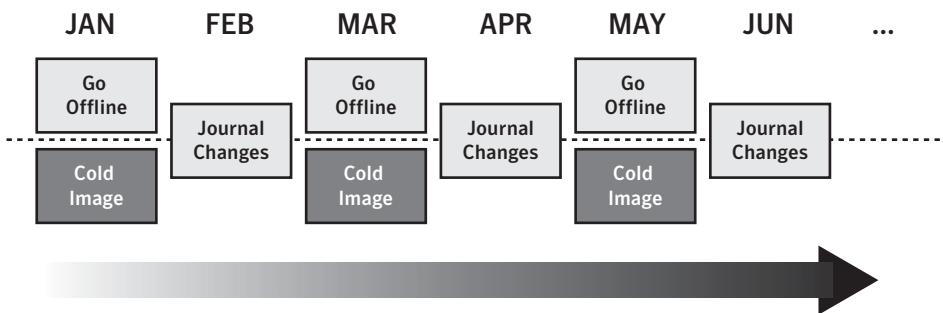


Figure 1. Traditional backup method

When preparing for bare metal recovery to dissimilar hardware, users will commonly keep a journal intended to account for each of the changes that have occurred on the computer. This manual method of bookkeeping is tedious and often fails to account for many system changes. In addition, some administrators will capture the most recent “cold image” of the system during the infrequent occasions when that system can be offline. These steps amount to a significant management effort just in planning for system recovery. And the result is still a painfully slow recovery.

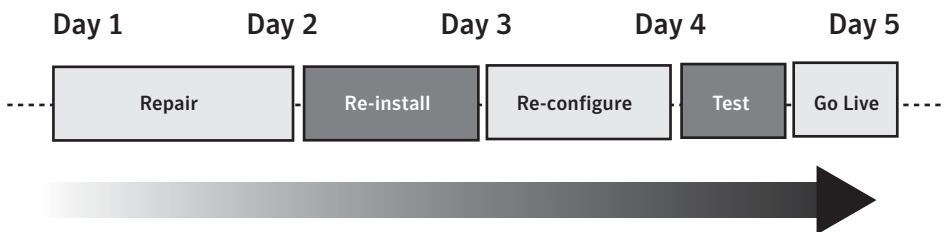


Figure 2. Traditional recovery method

Manual recovery relies on multiple steps following a layered approach that is intended to restore the system as closely as possible to its pre-failure state. If “cold images” were captured, then the most recent one can be recovered as a starting point. But all changes since the last image will still have to be accounted for manually.

Breaking Through the Dissimilar Hardware Restore Challenge

Duplicate hardware for disaster recovery

To hedge against hardware failure and still allow for automated system recovery, many organizations purchase duplicate hardware for the most critical computers. Imagine having a recovery time objective (RTO) that dictates full site recovery... at an alternate site...within a week...within three days...or even sooner. While not all organizations have this requirement, dissimilar hardware recovery is a concern for every administrator. As the RTO becomes compressed, the problem of dissimilar hardware is compounded and so is the cost. Maintaining duplicate hardware for an entire site is so cost-prohibitive that only the most critical (and a small percentage) of systems can justify this.

When purchasing duplicate hardware, system vendors often cannot guarantee that even the same model will have the same components from one batch to the next. It is not uncommon for a manufacturer to change a storage controller or other component as updated versions become available. This has implications for corporate purchasing policies because you must purchase computers all at once to assure that they have the same hardware components.

Hardware-independent restore, a critical component of system recovery

As stated earlier, restoration through layered reinstallation is a painful and time-consuming process. A typical Microsoft® Small Business Server with a small database application would take over four hours to reinstall—on a good day, if nothing went wrong and you paid attention the whole time. Using Backup Exec System Recovery (formerly LiveState Recovery), the process is just a couple of clicks away from automatic running and can take 30 minutes or less.

Breaking Through the Dissimilar Hardware Restore Challenge

Task	Manual	Recovery
BIOS, RAID configuration	:10	:10
OS installation from CD	:50	NA
OS updates	:30	NA
Application installation from CD	:15	NA
Application updates	:15	NA
System state and other unique system settings	:15	:20
Backup Exec System	2 Hrs 15 Min	30 Min

Table 1. Manual recovery vs. Backup Exec System Recovery

With the Restore Anywhere capability in Backup Exec System Recovery, it doesn't matter anymore which hardware the downed device is going to be restored to. There is no more need for layering a restoration because of hardware incompatibilities found during the restoration process.

The Restore Anywhere technology understands how to replace all the critical system drivers during a routine restoration. It also launches Windows native plug-and-play capabilities to detect additional non-critical devices and peripherals. The result is a fully functioning computer system on whatever hardware is available at the time of the recovery. You can restore the system not only to new hardware, but to a *virtual environment* as well.

The Restore Anywhere capability enabling recovery to dissimilar physical computers

Backup Exec System Recovery offers the first image-based dissimilar hardware system recovery on the market. The Restore Anywhere capability makes recovery to dissimilar hardware simple and reliable. With this capability, users are able to recover to completely different hardware. The most problematic elements of a system are handled easily. For example, with the Restore Anywhere capability, you can recover a single-processor computer to a multi-processor computer. You can recover from SCSI to SATA or SAS storage. Along with these changes, the Restore Anywhere capability enables recovery to different HAL, chipset, and kernel models.

"Being able to quickly, easily and consistently re-create a Windows system after a catastrophic failure has been all but impossible, until now. Symantec LiveState Recovery 6.0 not only makes it possible, it makes it a mandatory decision....The downtime LiveState Recovery can and will avoid will more than pay for the cost of the product."

*Steve Duplessie, Enterprise Strategy Group
Symantec's LiveState Recovery 6.0
Storage & Information Management Brief,
September 2005*

Breaking Through the Dissimilar Hardware Restore Challenge

Using the Restore Anywhere Capability

When it runs, Backup Exec System Recovery captures an entire system image called a “recovery point.” Recovery points can be set up in a scheduled job to occur automatically without any continuous intervention from the IT administrator. There are two types of recovery points that can be scheduled. A base only, or a base with incrementals. Best practices suggest that full system recovery points, called a “base,” be run during non-production hours or during times of lower system resource utilization. Incrementals can be scheduled to run during production times depending on the size of incrementals and the resource utilization settings for Backup Exec System Recovery.

Users should be aware of which drivers their systems are using and whether they are already supplied on the default Symantec Recovery Disk (SRD). This single CD is designed to recover all the computers in your environment. The CD already contains all the storage, HAL, and kernel drivers that Windows Server™ 2003 and Windows XP use when performing a new installation. In addition, Symantec has included a large number of drivers that are not part of the standard Windows installation media. Additional drivers can be added by the user or by Symantec to keep the CD up-to-date for all the systems that an administrator must support.

Recovering with Restore Anywhere

When Backup Exec System Recovery performs a bare metal restore, the SRD loads the necessary storage, HAL, kernel, and network drivers upon boot into a Windows-based environment called WinPE. A user then selects the desired recovery point and the destination, and then selects the option to restore to dissimilar hardware. The recovery proceeds to restore the entire system to unallocated space on the selected hard drive(s). Near the end of the recovery, Restore Anywhere will perform the retargeting process by automatically updating the storage, HAL, kernel, and other critical drivers for the system that was just restored. This process adds approximately 30 seconds to the recovery process. If these drivers or components are not already on the Symantec Recovery Disk CD, then the user will be prompted to supply them. The user can then place the driver in the same location that the recovery point is located since the SRD already has access to this location. From there the user simply browses to the drivers and installs them much the same as would be done in a native Windows driver installation.

Breaking Through the Dissimilar Hardware Restore Challenge

After this process the newly restored system will boot for the first time on the new hardware. Restore Anyware will initiate Windows plug-and-play to run during this first boot. Plug-and-play will take approximately 10–15 minutes. Once complete, the user can log in with either domain or local credentials and check the Device Manager for any non-critical components that plug-and-play did not detect.

Restore Anyware and recovery to virtual computer environments

Server and storage consolidation go hand in hand in today's data centers. Not only is central storage necessary for clustering and backup purposes, but centralized and consolidated servers also are reducing the hardware complexity of clustered systems. And the only way today to consolidate servers in a realistic way is through Virtual Server technology. Virtual Server Technology, such as VMware, is a software layer that enables the positioning of several virtual servers on a single physical server so that each virtual server can share the same physical resources without affecting each other. It allows up to 64 virtual servers per physical server, reducing hardware costs for hot standby servers, and keeps the number of servers manageable.

Normal Server	Virtual Server		
Exchange	Exchange	SQL Server	Web Server
	Windows	Windows	Windows
Windows	Virtual Server Virtualization Layer		
	Windows for Physical Server		
Hardware Architecture	Hardware Architecture		

Table 2. Physical server compared to virtual server

So instead of having multiple servers at a remote site, a single (albeit larger and faster) server can be deployed with multiple “virtual” hot standby servers running inside it.

With Backup Exec System Recovery, Symantec has partnered with VMware to provide rapid conversion of recovery point files to a VMware or VMDK file. This includes support for conversion of physical systems to virtual systems (P2V) and virtual systems to physical systems (V2P). VMware has also enabled the GSX Server 5.5 and Workstation 5.5 products to mount a Symantec recovery point using drivers provided by Symantec.

The conversion tool that Symantec provides as part of the Restore Anyware capability supports VMware Workstation and GSX Server version 5.0 or later. Similar processes can be used for converting to the VMware ESX platform and Microsoft Virtual Server platform, but these require additional steps and are not fully supported by Symantec.

Restore Anyware for hardware migration and hardware repurposing

Part of the lifecycle for Windows servers and desktops is migration. When hardware becomes outdated and is replaced, the system must be migrated. The migration process is equivalent in many ways to a bare metal recovery. It is even likely that your current strategy for migration closely resembles that for bare metal system recovery. Shortfalls of the process for bare metal recovery are also felt when performing regular migration processes. Using Backup Exec System Recovery with the Restore Anyware capability is an ideal solution to hardware migration woes. If you are already using it for bare metal system recovery, then it is a natural fit as the centerpiece of your hardware migration strategy as well.

Hardware migration strategies

Any migration procedure should define the reasons for migration, steps involved, fallback precautions, and other important factors that can influence the migration process. Two underlying philosophies influence technology upgrades, each philosophy working against the other. The first is the expression “If it ain’t broke, don’t fix it.” Obviously, if an organization has a functional, easy-to-use, and well-designed server infrastructure, upgrading may not be so appealing. The second philosophy is something along the lines of “Those who fail to upgrade their technologies perish.” But that means restoring each server to new hardware with new drivers and their peculiarities, and then cascading hardware upgrades “down the line” until all servers on the list are upgraded to the next highest level, with the bottom server being “dropped out of the pool.”

No matter which approach you take, the Restore Anyware capability will be a key factor in your hardware migration plan. Within the next three years, you will have a hardware failure or you will need to upgrade your hardware. Those are the facts of life. Here’s what to do when it happens.

Preparing a new system for migration

The migration process involves planning the migration, pilot testing the migration, migrating, and then planning for a short interim time for rollbacks if necessary. We won’t be able to cover the length and breadth of the entire migration process, but we can outline a few of the key portions of it and make clear how Symantec Backup Exec System Recovery with Restore Anyware can help.

Breaking Through the Dissimilar Hardware Restore Challenge

The first thing you'll want to do is to ensure that your Symantec Recovery Disk recognizes the storage controller(s) and NIC(s) in the new server, and that you have a backup of the native state of the new server. You'll need to install the Backup Exec System Recovery software onto the new server. During the process you'll be able to check the new computer's hardware for any drivers that the SRD CD may not have (step 1 in Figure 4). If new drivers are needed, send a request to Symantec support and they can update the CD for you or provide you the steps to do this on your own indicated by step 2 in Figure 4. You now have an updated universal SRD. With that in hand, you'll be able to create a base recovery point of the new server and store that file on the recovery point warehouse, along with the suggested configuration information worksheet for the server (step 3 in Figure 4).

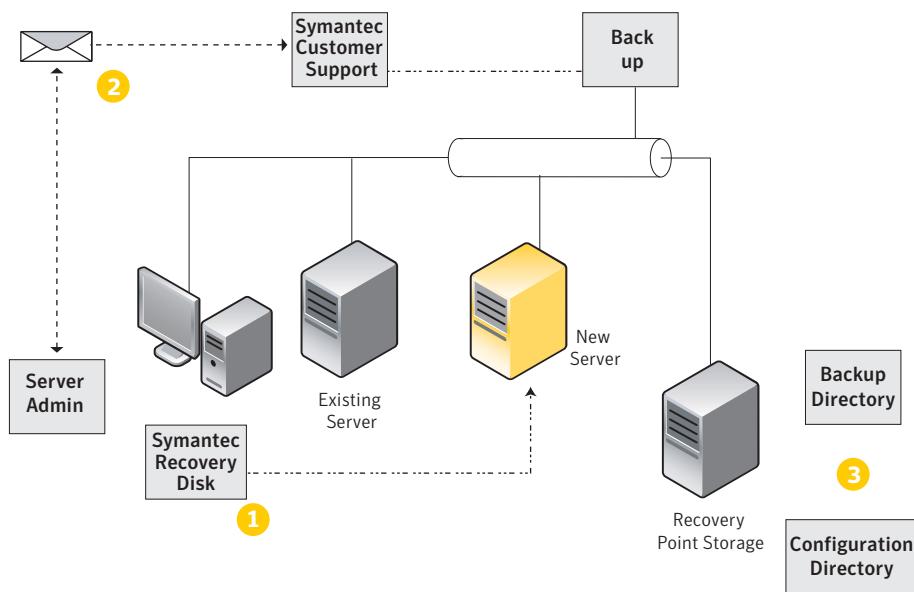


Figure 3. Upgrade Planning Sketchbook—Planning for Restore Boot CD

By preparing your new system this way, you'll have ensured that you can boot from the CD if necessary, that you have the configuration information to rebuild any portion of the system, and that you have a baseline recovery point you can always revert to if you encounter problems during migration.

The good news about a migration plan is that all new computer drivers can easily be added to the master SRD, and once added, the CD can be used on all subsequent servers already in place.

Repurposing hardware for optimal resource utilization

Similar to hardware migration, repurposing can be a valuable exercise when you determine that some servers are being underutilized while others are being overutilized. Most IT organizations have encountered the need to repurpose hardware at one time or another to make the best use of existing resources.

When integrating Backup Exec System Recovery and the Restore Anyware capability into the hardware repurposing process, you can ensure that your installation time for migrating from one platform to the next will be as quick as possible. As mentioned earlier, manual reconfiguration of a server is a multilayer process (configuring the RAID, etc.; installing the OS, service packs, patches and apps; configuring settings) involving as many as 90 steps that usually takes at least four hours of an administrator's time. Inserting Backup Exec System Recovery into the process reduces the time it takes for this by up to 80%. With Backup Exec System Recovery it is a four-step process. More importantly, the steps do not have to be journaled and can be replicated the same every time with no special training.

- 1.&2. Boot the server to be repurposed and ensure that the BIOS, and RAID configurations are set properly for the new system. This should take about 10 minutes.
3. Locate the recovery point from the existing server you are migrating from and restore it to the new server.
4. Back up the new server to a new directory, creating a recovery point in case you need to roll back to this point on the new server. Do not delete the old recovery point until you are sure that the migration has taken place successfully.

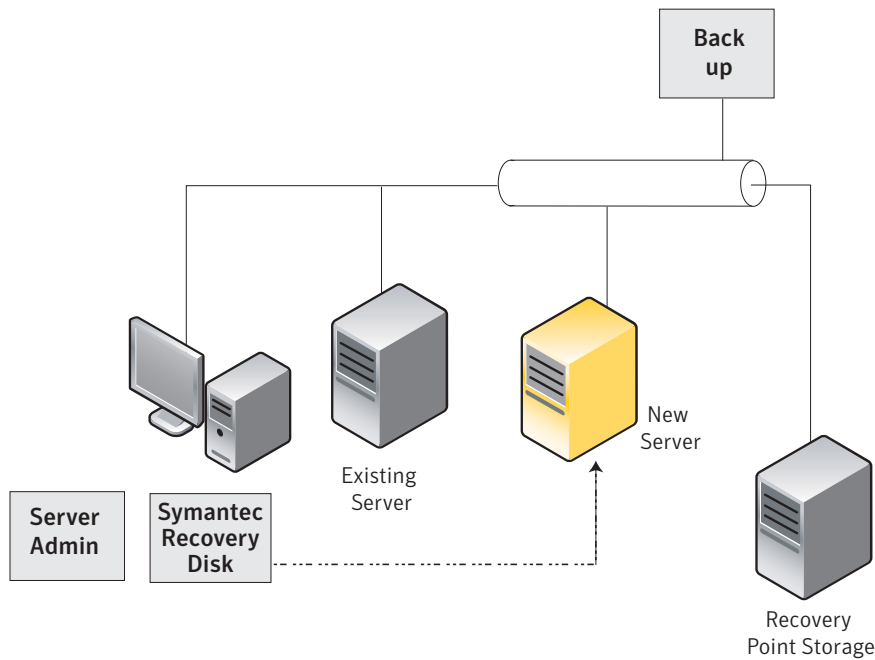


Figure 4. Upgrade Planning Sketchbook—Server Repurposing

A new option for meeting strict RTOs and upping disaster tolerance

Existing technology solutions provide many types of failover for the most critical systems. But there is a scarcity of solutions that provide rapid system recovery for computers that cannot justify the expense of high-end failover technologies. With Restore Anywhere technology, there is a new option for meeting stringent RTOs that do not require immediate failover. This provides a much-needed recovery solution for computers that cannot justify the high cost of clustering or mirror sites but must be recovered in minutes or hours. One factor in determining the appropriate solution is “disaster tolerance.”

Defining “disaster tolerance”

The recovery time objectives are very short for many organizations today. Too short to allow for ordering new computers and have them arrive in a couple of days or a week. To shorten the recovery time, you have to increase the disaster tolerance of the system. Disaster tolerance is the ability of a system to survive a disaster. In most cases, this means the ability to endure multiple points of failure. In an extreme case, this can include the loss of an entire data center or facility and all its functions. How can you make a server disaster-tolerant? The answer depends on the degree of tolerance to multiple failures you want to achieve. This in turn has financial consequences, because the most fault-resilient systems are also the most expensive. Each level of protection has its own requirements and associated costs and benefits. A common mirroring scenario is shown below.

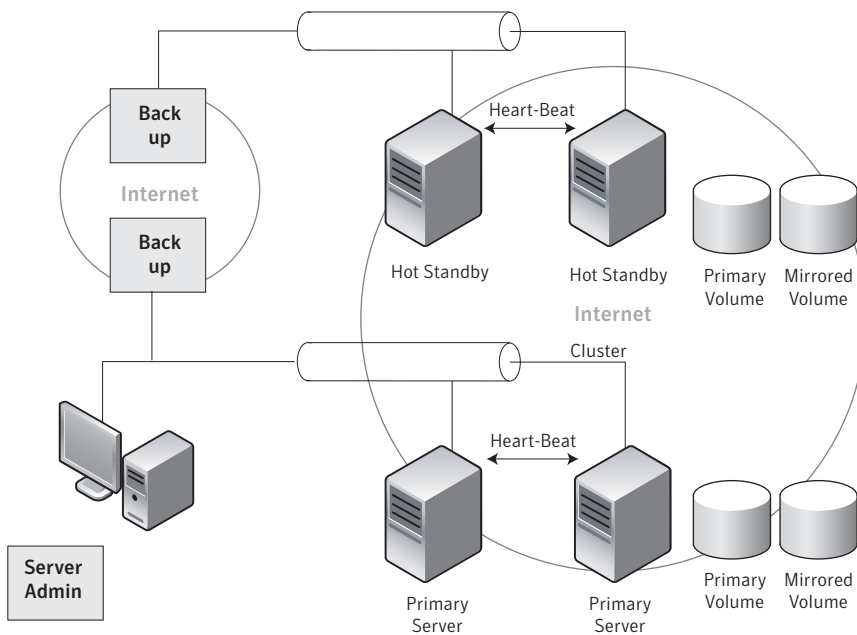


Figure 5. Server Backup Sketchbook—Backing up the mirrored server

What is your Recovery Time Objective (RTO)

Your specific RTO—the maximum amount of time it should take you to bring a service back online—will determine which of the approaches below you should consider.

Criticality	Recovery timeframe	Cost
Low	Systems do not need to be available for days or weeks; there is time to perform traditional manual or automated system reinstallation and recovery.	\$
Medium	Systems and replica sites must be available in minutes or hours; hardware does not need to be similar, or virtual systems can be used.	\$\$
High	Systems must failover immediately; replica sites with the same or similar hardware must be available for failover.	\$\$\$\$

Table 3. Criticality vs. cost

Many systems fit into the medium category for criticality but have not had a viable technology solution that made sense for the budget. The missing capability has been full, rapid recovery to dissimilar hardware. With the release of Backup Exec System Recovery and the Restore Anywhere capability, there is an answer for systems that must be recovered in minutes or hours to whatever hardware is available and even to virtual systems.

In fact, using Backup Exec System Recovery, administrators can achieve medium criticality objectives while costs remain comparable to low criticality approaches after factoring the manpower needed for manual reinstallation.

Conclusion

The Backup Exec System Recovery Restore Anywhere capability will dramatically change the way that organizations perform a wide-range of IT tasks, including bare metal system recovery, restoration to virtual environments, hardware migration, repurposing, change management, and site-level recovery. Using disk-to-disk technology, it enables organizations to meet ambitious recovery time objectives. And with breakthrough Restore Anywhere functionality, Backup Exec System Recovery provides even greater flexibility in recovering systems. It enables you to reduce recovery times and save significant hardware investments.

For more information about Backup Exec System Recovery and the Restore Anywhere capability, visit us online at www.backupexec.com.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries.

More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2006 Symantec Corporation. All rights reserved. Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Symantec Backup Exec System and Symantec LiveState Recovery are trademarks of Symantec Corporation. Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other brand and product names are trademarks of their respective holder(s). Printed in the USA.
05/06 10702267